# CHAPTER 6

BY

VISHU GOYAL

ETISHA JAIN

## ***LINUX 6.1 Understaning the Need for user Accounts***

- A user is a security principle, user accounts are used to provide people or processes access to system resources
- Processes are using system accounts
- People are using regular user accounts

***Linux 6.2 Userstanding User Properties***

- **cat /etc/passwd**

- **Name:** The name of the account
- **Password:** the secret that is used for authentication, may be disabled and also store in /etc/sudoers file
- **UID:** a uniquie identifier for users
- **GID:** the ID of the primary group
- **GECOS:** additional non- mandatory information about the user
- **home directory:** the environment where users create personal files
- **shell:** the program that will be started after successful authentication

eg: **student:x:1000:1000:decription:/home/student:/bin/bash**

***LINUX 6.3 Creating and Managing Users***

- **useradd --help | less**
- useradd : create a user account
- **useradd -C bill bill**
- -C it will help you to set the description of the user
- -p is used to set the passwd
- -s is used to set the shell
- usermod: modify user accounts
- **usermod --help | less**
- **usermod -aG wheel bill**
- **userdel:** use to delete the user accounts
- **userdel --help | less**
- -f forcefully
- -r for remove
- **userdel -rf bill** -> it will delete all the directory related to the account and also remove account
- **userdel -f bill** -> it will remove account only not directory becox user have done many things
- **passwd:** set passwd
- **passwd --help | less**
- **-**l lock
- -u unlock
- -e expire
- -S status
- **passwd bob**
- **passwd -l bob**
- **passwd -u bob**

## ***LINUX 6.4 Managing User Default Setting***

- use **useradd -D** to specify default setting
- **useradd -D** it show the default setting
- The default setting of the useradd is store in file /etc/default/useradd
- Files in **/etc/default/useradd** apply to useradd only if we change by default setting in this file then this will change for all the default user creating

- **cat /etc/default/useradd**
- # useradd defaults file
- GROUP=100
- HOME=/home
- INACTIVE=-1
- EXPIRE=
- SHELL=/bin/bash
- SKEL=/etc/skel **a directory which contents will be copied when new user created**
- CREATE_MAIL_SPOOL=yes

- alternatively, write default settings to **/etc/login.defs**
- **vim /etc/login/defs** it contains bydefault value to the new users if you changes the values of the users then it won't be affected to the old users

- PASS_MAX_DAYS
- PASS_MIN_DAYS
- PASS_MIN_LEN
- PASS_WARN_AGE

- UID_MIN
- UID_MAX

- GID_MIN
- GID_MAX

- CREATE_HOME  yes

- UMASK  very intersting topic

- **cd /etc/skel**  this is the directory which is used and put all the files which you want ot share with the newly user bydefault.
- ls -a
- **.bash_profile**  is used for configuration file that is used for process when the user is loggin in.
- **.bashrc** is the configuration file which is used to precessed while starting a new shell.

***LINUX 6.5 Understanding /etc/passed  and /etc/shadow***

- **/etc/passwd** is used to store user properties
- eg : **root:x:0:0:root:/root:bin/bash**
- **root** user have **UID is 0** becoz it doen't depends on the name of the user, it only depends on the user id.

- **NOTICE** shell is used for most of the system accounts
- **/sbin/nologin**  it is becoz system accounts have no business logging
- **/bin/syn**  it can run one task only
- **/sbin/halt**

- all the **ordinary user id** starts with the **1000**
- Password properties are stored in **/etc/shadow  (x)**

- **cat /etc/shadow**
- **root :  $kdjfowheoionewiei  :  :  0  :  99999  :  7  :  :  :**
- **2nd field**  it is not a password and not a encrypted passwd it is just a hash  that goes it
- After password field first four numbers are make sense and rest of the field are optional.
- 17912 is the first time when the password set in the universe( january 1st 1970) is epoch
- linux begining time is the **epoch time**
- 0 is the minimum validity of the password
- 99999 is the maximum amount of days
- 7 is the numbers of days before the warning will come to re-built new password
- if password field is empty then it means it is the disabled password

- if the user is locked then the password field will  show the ! **(exclamation sign)** that is user password can no longer be used, you can also remove the ! sign by using the vim

- **/etc/group**
- **root:x:0:**
- group name
- group passwd
- group Id
- the name of the members who is the member of its group

## ***LINUX 6.6 Understanding Group Membership***

- Each user must be a member of at least one group
- Primary Group Membership is manages through /etc/passwd
- The user primary group becomes group-owner if a user creates a file
- Additional (secondary) groups canm be defined as well
- Secondary Group Membership is managed through /etc/groups
- Use id to see which groups a user is a member of.

## ***Practical***

- **id demo**
- **usermode -aG wheel demo** it will add the group wheel to the demo
- **id demo**
- **grep linda /etc/passwd** it will show the primary group
- **grep linda /etc/group** it will show the secondary group

## *LINUX 6.7 Creating and Managing Groups*

- Use groupadd to add groups
- groupdel and groupmod can be used to delete and modify groups
- Use lid - g groupname to list all users that are member of a specific group

- **lid -g wheel**
- **grep wheel /etc/group**

***LINUX 6.8 Managing Password Properties***

- Basic password requirements are set in /etc/login.defs
- For advanced password properties, Pluggable Authentication Modules ( **PAM** ) can be used
- Look for the pam_tally2 module
- to change password settings for current users, use chage or passwd as root.

**Practical**

- **chage linda** it will ask several thing to change the setting of the password
- **grep linda /etc/shadow**
- **chage --help | less**
- **passwd --help | less**
- The difference in between both the command are : passwd provide us to delete or lock the passwd.

# THANK YOU